PROCEDURE 1410.17
Issued January 6, 1997

SUBJECT: Michigan State Government Network Security Policy

APPLICATION: Executive agencies and other non-executive branch entities which use the State data communication networks.

PURPOSE: Provide security policies and guidelines for State agencies, users and administrators of the State data communication networks.

CONTACT AGENCY: Department of Information Technology (DIT)
Research and Policy

TELEPHONE: 517/373-7326

FAX: 517/335-2355

CONTENTS:

1.0 SUMMARY:

The State data communication network is intended for conducting State business and exchanging information among State agencies, State employees, citizens and other stakeholders. This network was designed to be compatible with, and to have secure, controlled connection to the Internet. While this design offers significant new opportunities for customer and supplier interactions, it also brings serious concerns regarding network security. These guidelines address those security concerns and also define security responsibilities for DIT, agencies and users. This policy does not apply to voice or mainframe data networks not connected, in any way, to the State data network.

2.0 DEFINITIONS:

Security includes protection against: unauthorized access into systems; unauthorized modification of information; denial of service attacks; and information privacy violations.

State Data Communications Network is composed of a secured, internal network called an Intranet and an external, unsecured network, which is connected to the Internet. This network is comprised of necessary routing and switching hardware, software, wiring networks, connecting hub hardware, network management systems and the State firewall.

Intranet is the secured, internal network inside the firewall. It includes the core Lansing Metropolitan Area Network (LMAN), a Wide Area Network (WAN) connecting outstate locations, and agency local area networks, which are connected to either LMAN or WAN.

Unsecured network is an optical fiber network in greater Lansing, outside the firewall. It radiates from a switched Ethernet hub and is connected to the worldwide Internet.

Intranet servers conform with World Wide Web standards and are connected to the State Intranet, which is the secured, internal network segment located inside the firewall system.

Internet servers conform with World Wide Web standards and are connected to the State unsecured network outside the firewall, with unrestricted access to, and from, the Internet.

3.0 SECURITY PRINCIPLES AND RESPONSIBILITIES:

3.1 SECURITY PRINCIPLES -

Network security is a shared responsibility of DIT as network service provider, Agencies as information and local area network providers and Users of the State data network.

DIT will take all **reasonable** steps to make the State network perimeter as secure as possible. However, it is ultimately the responsibility of agencies to protect their systems, local area networks and information. Network security can range from unrestricted access to absolute security. This policy aims at achieving a **reasonable** balance between these two security extremes because State information primarily exists to serve State citizens.

Agencies are encouraged to make public information and business transactions available to State citizens and other stakeholders via policy-compliant Internet or Intranet servers.

3.2 DIT RESPONSIBILITIES -

DIT Infrastructure Services Telecom & Network Management is the State network service provider, responsible for efficient and secure operation of the State backbone network.

The Network Operations Center (NOC) has been delegated the responsibility for operating the State backbone data network and maintaining a security network perimeter. This security perimeter is defined by a firewall system which acts as a "wall" between a secured, internal Intranet and an unsecured, external network. This firewall, a network management system and connecting router hardware are the key tools for monitoring traffic, controlling access, and detecting unauthorized network intrusions, from the "unsecured" Internet into the secured internal (Intranet) network.

NOC also operates the Domain Name System (DNS) which is used by all Internet users to locate (resolve addresses for) State agency Intranet and Internet server resources. The State DNS is generally configured to prevent internal Intranet server addresses from being revealed to external non-State Internet users. Exceptions are listed in Section 5.5 below.

3.3 AGENCY RESPONSIBILITIES -

Agencies are responsible for the security of and access to agency program data, consistent with legislative or administrative restrictions. Agencies are also responsible for securely operating their own local area networks and servers. Unsecure operating practices, which expose other connected State networks to malicious security violations, are not acceptable.

Agencies must follow the Firewall Access Policy provisions (Section 4.3), if those servers require data or transactions which must pass through the State's secure firewall perimeter.
Agencies must coordinate with NOC to enter the proper pointers into the State Domain Name System (DNS) for identifying and locating their Intranet and Internet servers.

3.4 USER RESPONSIBILITIES -

Users are individually responsible for their own actions while using the state data communications network. They are responsible for complying with user provisions in this Network Security Policy and the State Acceptable Use Policy (Admin Procedure 1310.16).

Weakness in the security of a system is not a license to penetrate or abuse a system. Unauthorized access to a networked computer is explicitly a violation of the State Acceptable Use Policy. Likewise, users are prohibited from breaking into other user accounts or files without their permission or maliciously disrupting their service. Users are individually responsible for all network resources assigned to them; hence the sharing of accounts, passwords or assigned resources is prohibited. Users must power down their desktop PC workstations or log off from their local area network when leaving for the day.

4.0 DIT SECURITY GUIDELINES:

4.1 DIAL-IN SERVICE -
Dial-in access into any connected State network will only be permitted through centralized dial-in servers. These servers will provide the functionality to: 1) authenticate all remote dial-in users and 2) authorize their privileges, rights, and permissible actions in the use of specific network resources. In the case of dial-in access to extremely sensitive information, authentication may require the use of Digital Certificates (see Section 6.5). DIT will develop and publish standards for these dial-in servers. Until a centralized DIT dial-in facility is established, agencies may operate their own, policy-compliant, dial-in facilities.

The standard for dial-in access into centralized State dial-in servers are devices which support the Internet Point-to Point Protocol (PPP). PPP provides for the authentication of remote users and encapsulation of multiple local area network protocols.

This security policy explicitly prohibits any single connected State PC workstation from using Direct Inward Dial capability, inbound Facsimile or voice mail. These connections essentially circumvent the State firewall system and, therefore, constitute a potential threat to network security. After centralized servers for the above services are established, agencies must remove or disable existing PC-based dial-in products. In addition, networked State PCs, with dial-out modem capability, must disable the Auto-Answer feature. Agencies, which have limited and legitimate uses for PC-based dial-in, may describe the need and request exception through the DIT Telecommunications Requirements Analysis Document (TRAD) process - Administrative Procedure 1410.09.

4.2 INTRUSION DETECTION AND RESPONSE -
DIT, in collaboration with the Network Security Administrators Committee will develop a plan for network intrusion detection and response, analogous to a disaster recovery plan. The plan will include means for reporting intrusion, categorizing levels of incidents, guidelines for response escalation and a hierarchy for elevating decisions. Appropriate responses to intrusions/threats to network security may include changing user passwords, using encrypted data techniques, interrupting service or possibly disconnecting systems or networks. Any of these possible responses will be closely coordinated with agencies so as to minimize the impact on network operational readiness. Intrusions involving possible violations of State or Federal law will be reported to the proper authority.

4.3 FIREWALL ACCESS POLICY -
The State firewall is capable of prohibiting access into and restricting traffic between the State's internal, secured Intranet and its external, unsecured network. The firewall is key to establishing a secure network perimeter and to managing secure access into agency data.

The firewall has been initialized to restrict all packet traffic coming from the Internet, with the exception of E-mail, DNS and World Wide Web traffic. No restrictions are generally made on internal TCP/IP traffic outbound to the Internet. However, the firewall is very flexible in its ability to screen and restrict most types and sources of inbound or outbound Internet traffic, including World Wide Web pages and Browser-activated Java applets.

DIT will give primary consideration to agency needs for data exchange through the firewall into agency Intranet servers or into proxy database servers. However, DIT must balance those agency needs with an acceptable level of risk for network security.

Agencies currently must use one of three methods for authenticated remote user access through the firewall - Internet Source/Destination Address; S-key and Secure ID, which is the preferred method. Agencies must coordinate with Telecommunications Services their needs for authenticated access and for restricting agency traffic through the firewall via the DIT TRAD process.

5.0 AGENCY SECURITY GUIDELINES:

5.1 AGENCY NETWORK SECURITY ADMINISTRATOR -
Agencies must designate an Agency Security Administrator responsible for coordination of technical security issues concerning agency networks, Intranet and Internet servers. This person must be a member of the Agency Network Security Administrator Committee.

5.2 AGENCY NETWORK SECURITY ADMINISTRATOR DUTIES -

- Primary contact for agency security and Intranet/Internet server issues.
- Representative to the Network Security Administrators Committee.
- Ensure compliance with State's Security and Intranet/Internet Policies.
- Coordinate with NOC any proposed changes in network topology.
- Ensure that any agency connection(s) to State unsecured network is isolated from any agency local area network or from the State Intranet.
- Remove existing remote dial-in access software from each agency PC.
- Eliminate unauthorized agency external (back door) connections.
- Prepare and submit a TRAD for future agency external connection needs.
- Keep aware of security issues by subscribing to security news groups such as Computer Emergency Response Team of Carnegie-Mellon University.
- Strive for continuous improvements in network security.

5.3 AGENCY NETWORK SECURITY ADMINISTRATORS COMMITTEE -
DIT will established this committee to address all technical aspects of State network security. It will be comprised of a Telecommunications Services representative and all Agency Network Security Administrators and will be chaired by Telecommunications Services.

This committee's activities and responsibilities will include:

- Addressing network security threats.
- Addressing network security operational issues such as: intrusion detection and lockout, administering user accounts, passwords and logs, system monitoring, system back-ups, physical site security, etc.

- Ensuring that agency security administrators are kept current on security policies, procedures and activities.
- Design and conduct effective security awareness and training programs.

5.4 OPERATIONAL GUIDELINES FOR INTERNET SERVERS -
Internet servers are intended to provide public information and agency business transactions to the public and other stakeholders via the Internet. These servers generally must be connected to the greater Lansing unsecured network segment via a Simple Network Management Protocol manageable Ethernet hub.

Agencies planning on Internet servers must follow State Internet server operation guidelines. They are responsible for operating those servers in a manner which will not adversely impact the security perimeter or servers attached to the State Intranet. Agencies must assure that no cross-connection is made between Internet servers attached to the unsecured network and the State internal secured Intranet.

Internet server-based dynamic business transactions, requiring access to specific internal Intranet-connected databases, will generally be accommodated with access through the Firewall. These agency applications must be requested via a TRAD.

Agencies which contract with private contractors to implement and operate off-site Web servers are generally restricted to providing static Web page information. Dynamic Web transactions, which require access through the firewall into internal State databases, will generally not be permitted on contractor-operated servers. An exception is when the agency's application database is tightly integrated with the contractor-operated Web server and is external of the State data network.

Outside contractors will generally be permitted only limited and restricted access into the State internal secured Intranet. Refer to Section 6.2 and 6.3 below.

5.5 OPERATIONAL GUIDELINES FOR INTRANET SERVERS -
Intranet servers are primarily intended to serve the internal information and business transaction needs of State workers. Intranet servers should also be used to streamline the internal operation and administration of State agencies.

Intranet servers generally should not be used to support the information and business transaction needs of the general public or non-State entities.

On an exception basis, agency Intranet servers may be accessed by special well-defined groups of remote Internet-based stakeholders. These non-State groups must use one of the accepted methods for authenticated access through the firewall. Business transactions, from these remote groups, will be restricted to only accessing limited and clearly defined agency Intranet servers. Agencies must use the TRAD process to describe and request approval for these applications.

6.0 GENERAL SECURITY GUIDELINES:

6.1 EXTERNAL CONNECTION POLICY -

The State data communications network was designed to have secure, controlled connections to the Internet. Some agencies have established Internet and other "back door" connections to remote users which by-pass the firewall. Examples are:

- Private line connections into agency servers for use by users or contractors
- Point-to-point connections with other State agencies.
- Connections to external service providers in support of agency programs.
- Connections to non-State Internet service providers or vendors

These connections are potential threats to the network for secure operation and for its operational integrity because of the potential for routing loops. DIT has the authority to examine existing connections and require agencies to remove them, if they are determined to present unreasonable threats to security or operational integrity. Agencies must submit a TRAD for future external connection requests.

6.2 CONTRACTOR SERIAL LINE INTRANET ACCESS SERVICE -

It is recognized that some agency contractors, in order to accomplish their State obligations, must have remote serial-line access into Intranet-attached resources.

To securely accommodate these serial-line remote-access needs, DIT has established a special network segment service. This segment, located outside the firewall, is equipped with a multi-port, serial-line router for attaching dedicated, private phone lines. It is designed to allow remotely-located contractors access through the firewall but restricted to accessing only designated internal resources. Agencies must describe the need and request these services via the TRAD process.

Contractors, approved for using this serial line access service, must comply with the conditions for network access for Non-State Entities listed in Section 6.3 below.

6.3 NETWORK ACCESS FOR NON-STATE ENTITIES

The preferred method, for non-State entities, to exchange information or transact business with the State is via Internet servers connected to the unsecured network.

Agencies may optionally request internal network access privileges for contractors or temporary employees who are under contractual, legal or administrative obligation to perform state government functions, provided that those entities are:

- Informed of, and sign an agreement to conform with both the State Acceptable Use Policy and this State Network Security Policy.

- Authenticated via assigned UserID and passwords at either:
  - an Internet server connected to the unsecured network;
  - a centralized dial-in facility or at the State firewall.
- Restricted to access only those data resources necessary to accomplish their assigned contractual duties.
- Granted access only for the term of their contract and are re-certified for access, at a minimum, annually.

6.4 COOPERATIVE SECURITY MEASURES -
Agencies and agency users shall practice cooperative security measures. Each site is responsible for notifying and assisting other sites in the detection of security violations. The Agency Network Security Administrator Committee will guide and facilitate these cooperative measures. Assistance may include tracing connections, tracking violators and cooperating with law enforcement officials. Security flaws attributable to vendor systems or software should be reported to other users and the vendor for timely corrective action.

6.5 ENCRYPTION POLICY -
Given the threat from users inside the firewall and those posed by external, determined and knowledgeable hackers, Agencies may, at their discretion and upon approval by DIT, employ data encryption techniques to protect the confidentiality or prevent the disclosure of data

Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Public Key Encryption are three techniques for transforming information from readable into unreadable formats. These techniques all use "keys" to encrypt data on a computer system or in transit across a network. DES and IDEA both use one key and special algorithms to encrypt and decrypt text. Several highly secure encryption systems use Public Key Encryption, which uses two keys; one public, widely known key to encrypt messages and a second private key to decrypt them.

Agencies, which require private transactions or secure transmission of data between their internal, networked personal computers or between hosts external to the State Intranet, may choose among several encryption technologies. Secure Sockets Layer (SSL) is one widely used technique for both securing information exchange and for authenticating remote users and Internet servers. SSL supports encryption of data based on public key encryption technology and the use of ITU Standard X.509 Public Key Certification Authorities (CA). Agencies may contract with private CA service contractors on a yearly basis until DIT offers that service.

Agencies, which must have assurance that data/information is securely received or transmitted without modification, may employ such cryptographic techniques as Message Digest-5 (MD5) Algorithm and Digital Signature Standard.

Agencies which accept credit cards for monetary business transaction via Internet or Intranet servers, must consider security techniques, such as SSL or Secure Electronic Transactions (SET). The use of encryption technologies for achieving data privacy, E-mail privacy, user authentication, protection of customer credit cards or establishing private virtual networks must be described and approved via the DIT Research and Policy RAD process (Administrative Procedure 1310.11).

Encrypted data, which is subject to public release and is requested under Public Act 442, the Freedom of Information Act, must be converted back to clear, unencrypted text.

Agencies and Users must comply with current Federal Government regulations on export and import of advanced encryption technology outside the US and Canada.

6.6 PASSWORD POLICY -

Users are expected to handle account privileges in a responsible manner and follow site procedures for the security of their data as well as that of agency systems. All agencies and their network users must follow the password guidelines outlined below. Agencies are responsible for defining and maintaining appropriate methods for file protection and server access control.

A necessary component of agency account management is password assignment policy. Passwords represent a security risk and perhaps are the most vulnerable part of any computer system. Intruders/attackers use sophisticated password guessing programs that involve large dictionary searches and algorithms to discover passwords. The following represent three levels of password security policy (minimum, normal or high) which agencies may choose:

	MINIMUM SECURITY	NORMAL SECURITY	HIGH SECURITY
password composition	digits (0-9)	Upper (A-Z, lower (a-z)	full 95 ASCII
password length	4-6 characters	4-8 characters	6-8 characters
frequency of change	once per year	twice per year	monthly.

It is recommended that agencies use high security password profile of a mix of 6-8 alpha and digit ASCII characters, but may change user passwords at least once every six months and not reuse those password until 3 password change cycles.

The following are password guidelines to avoid:

- DON'T use common words in proper or reverse spelling
- DON'T use common computer acronyms like SQL, DBMS,
- DON'T use names of famous or fictitious people
- DON'T use your login name in any form (as is, reversed)
- DON'T use your first, middle, or last name in any form
- DON'T use your spouse's or child's name
- DON'T use easily obtained numbers such as telephone, street, social security, etc.

- DON'T use password of all digits or starting with a digit
- DON'T write your password on paper affixed to desk or PC

The following are password guidelines to use:

- USE passwords of eight, or greater, characters
- USE eight or more letters alternating consonant and vowel
- USE a password with mixed-case characters
- USE a password with some digit and special characters
- USE a password that is easily remembered and typed
- USE two short words with a separating minus sign
- USE the first letters of the words from a favorite song or poem

7.0 PROCEDURES**:**

7.1 FOR DIT, AGENCIES and USERS -
Network security is the shared responsibility of DIT as a network service provider, State Agencies as information providers and Users of the State data communication network. They collectively have the shared responsibility for detecting and preventing security violations, identifying unauthorized intrusions and promptly responding to intrusions.

7.2 FOR DIT -
DIT is responsible for maintaining a secure network perimeter and the efficient and secure operation of the State's backbone data communication network, including routers, hubs, switching hardware, domain name service and also centralized network servers for E-mail, FAX, GroupWare, directory, public key certification and video conferencing.

DIT will conduct periodic security audits to assure compliance with this policy and also use tools to scan the State Intranet for intrusions and security vulnerability. DIT also will monitor network utilization to assure adequate capacity to meet user bandwidth demands.

DIT Telecom & Network Management will assist agencies in establishing and coordinating secure access through the firewall. They will assist agencies in the preparation of TRADs requesting authenticated access through the firewall. Telecommunications Services will respond to agency TRAD requests within 10 days.

DIT Research and Policy will maintain this policy to be in conformance with relevant administrative directives, Michigan laws and advances in security technology. It will be reviewed annually and will be re-issued when revisions are necessary.

7.3 FOR AGENCIES -
Agencies are responsible for securely operating their own local area networks and servers.

Agencies must designate an Agency Security Administrator responsible for coordination of technical security issues concerning network, Intranet and Internet servers.

7.4 FOR USERS -

Users are individually responsible for their own actions while using the state data communication network. They are responsible for compliance with the user provision listed in this Network Security Policy and in the State Acceptable Use Policy.

* * *